秘密分散法とそのバリエーション (符号と暗号の代数的数理)

AUTHOR(S):

山本, 博資

CITATION:

山本, 博資. 秘密分散法とそのバリエーション (符号と暗号の代数的数理). 数理解析研究所講究録 2004, 1361: 19-31

ISSUE DATE:

2004-04

URL:

http://hdl.handle.net/2433/25254

数理解析研究所講究録 1361 巻 2004 年 19-31

秘密分散法とそのバリエーション

東京大学・大学院情報理工学系研究科　山本 博資 (Hirosuke Yamamoto)
Graduate School of Information Science and Tecnology
University of Tokyo

1. はじめに

今日の情報化社会においては，ほとんどあらゆる情報がディジタル化され，計算機で処理されると共に，それらの情報はハードディスクなどの記憶装置に保管されている．そのような情報には，国や地方自治体の住民情報，銀行口座情報，企業の業務情報など，重要な秘密情報を含んでいる場合が多く，その安全な保管技術が必要不可欠である．しかし，ハードディスクなどの記録装置は故障する可能性があり，また，火事や地震あるいはテロなどにより記憶装置が破壊されてしまうこともある．

破壊や故障などで記録情報が取り出せなくなる危険性は，記憶装置を多重化し，それらに同じ秘密情報を記録しておくことで防ぐことができる．この危険性をできる限り軽減するためには，そのようなバックアップ用の記憶装置を，互いに離れたところに多数用意することが望まれる．しかし，秘密情報が異なる場所に多数存在することは，情報の漏洩の可能性を逆に増すことになる．破壊や故障の脅威からは秘密情報のコピー数を多くしたいが，漏洩の脅威からは秘密情報のコピー数を少なくしたいということになる．この相反する要求を同時に満たすために考案された符号化方式が秘密分散法 (Secret Sharing Scheme) である．

秘密分散法では，秘密情報 S を n 個の分散情報 (share)$W_j, j = 1, 2, \cdots, n$, に分散符号化する．(k, n) しきい値型の秘密分散法では，n 個の分散情報のうちから任意の k 個の分散情報を集めれば秘密情報 S が復号できるが，任意の $k-1$ 個の分散情報からは，S の情報が全く得られない特徴を持っている．したがって，(k, n) しきい値秘密分散法を用いれば，$k-1$ 個の分散情報が盗まれても，S の情報は全く漏洩しない．また，$n-k$ 個の分散情報が破壊されても，残りの k 個の分散情報から秘密情報 S を復元できる．このように，秘密分散法は，漏洩にも破壊や故障にも安全な情報の記録システムを実現できる．

本稿では，秘密分散法のバリエーションと，それらの実現法に関して紹介を行う．

1　秘密分散法の分類

秘密分散法は，最初 Shamir[1] により提案され，Karnin ら [2] により，情報理論的な解析が行われた．その後，秘密分散法に関して，非常にたくさんの研究がなされているが，秘密分散法は大きく表 1 のように分類できる．

通常の秘密分散法では，ある有限体上で表現可能な離散データを秘密情報とし，符号化復号化処理は計算機上で行われる．これに対して，秘密関数分散法 [3], では，秘密情報が有限体上の関数に拡張されている．また，視覚復号型秘密分散法 [4] では，秘密情報が

画像であり，復号に人間の視覚を利用するため，復号処理に全く計算機を必要しないという特徴がある．同様に，オーディオ秘密分散 [5] では音と人間の聴覚を利用している．

量子秘密分散法では，分散情報として量子状態を利用するが，量子状態がコピーできないという no-cloning theorem など，量子特有の条件を考慮して符号化復号化処理をしなければならない．また，量子秘密分散法では，秘密情報として古典的な通常のディジタル情報を符号化する場合と [6][7]，量子状態そのものを秘密情報とする場合 [8][9] とに分類できる．

(k,n) しきい値法では，任意の k 個の分散情報から秘密情報 S が復元でき，任意の $k-1$ 個の分散情報からは S が全く分からないという特徴を持つ．このように「しきい値型」では，秘密情報 S に対するアクセス構造が，分散情報の個数で決まっている．しかし，より柔軟なアクセス構造を実現したい場合もある．アクセス構造により秘密分散法を分類すると表 2 のように分類できる．しきい値型でないアクセス構造を，一般アクセス構造 (general access structure) という [10][11].

分散情報の集合うち，秘密情報 S を復号できるものを有資格集合 (qualified set) といい，S について全く情報が得られないものを禁止集合 (forbidden set) という．分散情報の全ての部分集合が，有資格集合または禁止集合のどちらかに所属するようなアクセス構造を完全 (perfect) であるという．これに対して，有資格集合でも禁止集合でもない中間的な集合（つまり，秘密情報 S を完全には復号できないが，S について何らかの情報が得られるような分散情報の集合）を許すアクセス構造を，ランプ (ramp) 型であるという [12][13][14].

表 1 の全ての秘密分散法に対して，表 2 のアクセス構造を考えることができ，その組み合わせ分のバリエーションが存在する．以下の節では，その幾つかを紹介する．なお，表記を簡単にするため，以下では秘密分散法 (Secret Sharing Scheme) を SSS と略記する．

表 1: 秘密分散法の分類

名前	秘密情報	復号	分散情報
(通常の) 秘密分散法	離散データ	計算機	数値データ
秘密関数分散法	離散的な関数	計算機	数理データ
視覚復号型秘密分散法	画像	人間の視覚を利用	画像
オーディオ秘密分散法	音	人間の聴覚を利用	音
量子秘密分散法 (1)	離散データ	量子測定/量子計算機	量子状態
量子秘密分散法 (2)	量子状態	量子計算機	量子状態

2 しきい値型秘密分散法

秘密情報 S および分散情報 W_j が，ある有限体 GF(q) 上の値を取るものとする．S が GF(q) 上の確率変数であるとき，分散情報 W_j も確率変数となる．これらの確率変数を用いて (k,n) しきい値型 SSS は次のように定義される．

表 2: アクセス構造の分類

	しきい値型	非しきい値型
完全	(k,n) しきい値型	一般アクセス構造
ランプ型	(k,L,n) しきい値型	ランプ型一般アクセス構造

定義 1 秘密情報 S の分散情報 $(W_1, W_2, \cdots W_n)$ が次の 2 条件を満たすとき，(k,n) しきい値型 *SSS* という．

1. 任意の相異なる k 個の分散情報 $W_{j_1}, W_{j_2}, \cdots, W_{j_k}$ から S が正しく復号できる．つまり次式が成り立つ．

$$H(S|W_{j_1}, W_{j_2}, \cdots, W_{j_k}) = 0 \tag{1}$$

ここで，$H(\cdot|\cdot)$ は Shannon の条件付きエントロピーである．

2. 任意の $k-1$ 個の分散情報 $W_{j_1}, W_{j_2}, \cdots, W_{j_{k-1}}$ からは，S の情報が全く得られない．つまり次式が成り立つ．

$$H(S|W_{j_1}, W_{j_2}, \cdots, W_{j_{k-1}}) = H(S) \tag{2}$$

この (k,n) しきい値型 SSS に対して，次の定理が成り立つ．

定理 2 (k,n) しきい値型 *SSS* において，任意の分散情報 W_j のエントロピー $H(W_j)$ は次式を満たさなければならない．

$$H(W_j) \geq H(S) \tag{3}$$

(証明)

分散情報 W_j および $m-1$ 個の W_{i_ℓ} が全て相異なる場合，次のように $H(W_j)$ の下界が求められる．

$$\begin{aligned} H(W_j) &\geq H(W_j|W_{i_1}, W_{i_2}, \cdots W_{i_{m-1}}) \\ &\geq H(W_j|W_{i_1}, W_{i_2}, \cdots W_{i_{m-1}}) - H(W_j|W_{i_1}, W_{i_2}, \cdots W_{i_{m-1}}, S) \\ &= I(S; W_j|W_{i_1}, W_{i_2}, \cdots W_{i_{m-1}}) \\ &= H(S|W_{i_1}, W_{i_2}, \cdots W_{i_{m-1}}) - H(S|W_{i_1}, W_{i_2}, \cdots W_{i_{m-1}}, W_j) \\ &= H(S) \end{aligned} \tag{4}$$

ここで，最後の等式は式 (1)(2) による． □

次に，式 (3) の等号を達成する SSS の構成法を考える [2].

秘密情報 S から分散情報 $W_1, W_2, \cdots, W_n$ を次のような線形演算で作る場合を考える．GF(q) 上の $k-1$ 個の独立な乱数を $U_1, U_2, \cdots, U_{k-1}$ とし，それと秘密情報 S をあわせた

横ベクトルを $\boldsymbol{U} = (S, U_1, U_2, \cdots, U_{k-1})$ とする．この $\boldsymbol{U}$ に $k \times (n+1)$ 行列 G をかけあわせることにより，分散情報 $\boldsymbol{W} = (S, W_1, W_2, \cdots, W_n)$ を

$$\boldsymbol{W} = \boldsymbol{U}G \tag{5}$$

で生成する．

式 (5) を用いて (k, n) しきい値 SSS を構成するためには，G の任意の k 個の列ベクトルが線形独立となるような行列 G を使用すればよい．いま，有限体 GF(q) の原始元を α とすると，

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & \alpha & \alpha^2 & \cdots & \alpha^{q-1} \\ 0 & 0 & \alpha^2 & \alpha^4 & \cdots & \alpha^{(q-1)2} \\ & & & & & \\ 0 & 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \cdots & \alpha^{(q-1)(k-1)} \end{bmatrix} \tag{6}$$

で与えられる行列 G は，任意の $k \times k$ の小行列の行列式が Vandermonde の行列式となるため，G の任意の k 個の列ベクトルが線形独立となる．したがって，式 (6) の G を用いれば，(k, n) しきい値 SSS を作ることができる．

式 (6) の第 2 列目を取り除いた G を用いると，各分散情報 W_j, $j = 1, 2, \cdots, n$ は $k-1$ 次の多項式

$$D(x) = S + U_1 x + U_2 x^2 + \cdots + U_{k-1} x^{k-1} \tag{7}$$

を用いて[1]，$W_j = D(\alpha^j)$ と表現でき，Shamir の多項式を用いた SSS[1] となる．

この場合，$y = D(x)$ の y 軸切片が秘密情報 S を与えており，(k, n) しきい値 SSS の原理は次のように説明できる．k 個の分散情報 $D(\alpha^j)$, $j = 1, 2, \cdots, k$, が集まると，$k-1$ 次の多項式 $y = D(x)$ の k 個の座標点 $(\alpha^j, D(\alpha^j))$ から $y = D(x)$ が一意に定まる．その結果，秘密情報の y 切片の値も求まる．しかし，$k-1$ 個の座標点からは多項式が一意に定まらず，全ての y 切片を通る可能性が等確率で存在するため，秘密情報 S が求められない．

定理 2 より，分散情報 W_j のサイズは秘密情報 S のサイズより小さくできず，n 個全部の分散情報のサイズは元の秘密情報の n 倍となり，符号化効率が悪い．

この欠点を改善するために考案されたのが，しきい値ランプ型 SSS である [12][13][14].

定義 3 秘密情報 S 対する n 個の分散情報を $(W_1, W_2, \cdots W_n)$ とする．このとき，任意の $l (0 \leq l \leq L)$ に対して，$k-l$ 個の相異なる分散情報 $W_{j_1}, W_{j_2}, \cdots, W_{j_{k-l}}$ が次式を満たすとき，(k, L, n) しきい値ランプ型 *SSS* という *[13]*.

$$H(S|W_{j_1}, W_{j_2}, \cdots, W_{j_l}) = \frac{l}{L} H(S) \tag{8}$$

式 (8) より，k 個の分散情報が集まると S が完全に分かり，$k-L$ 個の分散情報からでは S の情報は全く得られない．$k-L+1$ 個から $k-1$ 個の間の場合は，分散情報の増加に伴って，S に関して得られる情報が増えていく特性を持つ．

この $(k, L.n)$ しきい値ランプ型 SSS は，次の定理が成り立つ [13].

[1]演算は GF(q) 上の演算である．

定理 4 (k, L, n) しきい値ランプ型 *SSS* において，任意の分散情報 W_j のエントロピー $H(W_j)$ は次式を満たさなければならない．

$$H(W_j) \geq \frac{1}{L} H(S) \tag{9}$$

定理4より，(k, L, n) しきい値ランプ型SSSを用いれば，$L = 2$ の場合でも分散情報のサイズを $1/2$ にすることができ，符号化効率を大きく改善できる．また，S のサイズが大きい場合，$(1/L)H(S)$ も十分大きくなり，ランプ型を使用しても，分散情報が k 個より少ない場合に実用的に安全となるようにすることができる．

式(9)を等号で達成するランプ型SSSは，秘密情報 S を $S = (S_0, S_1, \cdots, S_{L-1})$ と L 個に分割し，式(5)または(7)の乱数 U_m のうち，$L-1$ 個の乱数を秘密情報 S_m で置き換えることにより実現できる [13]．

3 一般アクセス構造を持つ秘密分散法

前節ではしきい値型の秘密分散法の構成法を示したが，本節では，しきい値型の秘密分散法を利用して，一般アクセス構造を持つ秘密分散法を構成する方法を紹介する．

分散情報全体の集合を $\boldsymbol{V} = \{V_1, V_2, \ldots, V_n\}$ とし，秘密情報 S に対する有資格集合族を $\mathcal{A}_1$，禁止集合族を $\mathcal{A}_0$ で表す．このとき，与えられたアクセス構造 $\Gamma = \{\mathcal{A}_1, \mathcal{A}_0\}$ に対して，S を秘密情報に持つ (t, m) しきい値SSSを考え，その分散情報 $\boldsymbol{W} = \{W_1, W_2, \ldots, W_m\}$ を用いて，式(11)-(13)を満たす複数割当写像 $\alpha_\Gamma : \boldsymbol{V} \to 2^{\boldsymbol{W}}$ を構成する．ただし，$\boldsymbol{A} \subseteq \boldsymbol{V}$ に対して，

$$\alpha_\Gamma(\boldsymbol{A}) = \bigcup_{V \in \boldsymbol{A}} \alpha_\Gamma(V) \tag{10}$$

と定義する．

$$|\alpha_\Gamma(\boldsymbol{A})| \geq t, \quad \text{if } \boldsymbol{A} \in \mathcal{A}_1 \tag{11}$$

$$|\alpha_\Gamma(\boldsymbol{B})| \leq t-1, \quad \text{if } \boldsymbol{B} \in \mathcal{A}_0 \tag{12}$$

$$\alpha_\Gamma(\boldsymbol{V}) = \boldsymbol{W} \tag{13}$$

この写像 α_Γ を用いて，各分散情報 $V_i \in \boldsymbol{V}$ に $\alpha_\Gamma(V_i)$ を割り当てることにより，アクセス構造 Γ を持つSSSを構成することができる [10][11]．

(t, m) しきい値SSSの分散情報 W_j を，アクセス構造 Γ に対する分散情報 V_i と区別するために，W_j を基本分散情報と呼ぶ．基本分散情報 W_j のレートは，秘密情報 S のレートと同じ値まで小さくできるため，上記の複数割当写像を用いた場合，分散情報 V_i の平均レート $\tilde{\rho}$ と最悪レート ρ^* は，次式で与えられる．

$$\tilde{\rho} = \frac{1}{n} \sum_{i=1}^{n} |\alpha_\Gamma(V_i)| \tag{14}$$

$$\rho^* = \max_{1 \leq i \leq n} |\alpha_\Gamma(V_i)| \tag{15}$$

複数割当写像を与える簡単な方法としては，(n,n) しきい値SSSを用いて複数割当法を実現するcumulative map[10][11]や，それを改良し，(k,n) しきい値SSSを用いて複数割当法を実現する改良cumulative map[15]が知られている．しかし，それらのcumulative mapを用いる複数割当写像は一般にかなり効率が悪い．これに対して，以下では，平均レートまたは最悪レートを最小とする最適な複数割当写像を，整数計画を用いて求める我々の方式[16][17]を紹介する．

複数割当写像 $\alpha_\Gamma : \boldsymbol{V} \rightarrow 2^{\boldsymbol{W}}$ に対して，2^n 個存在する $\boldsymbol{W}$ の部分集合 $\boldsymbol{X}_{[k]_2^n}$，$k = 0,1,2,\ldots,N$ を，次式で定義する．

$$\boldsymbol{X}_{[k]_2^n} = \left[\bigcap_{i:[k]_2^{n,i}=1} \alpha_\Gamma(V_i)\right] \cap \left[\bigcap_{i:[k]_2^{n,i}=0} \overline{\alpha_\Gamma(V_i)}\right] \tag{16}$$

ここで $N = 2^n - 1$，$[k]_2^n$ は非負整数 k を n ビットの2進数表示したもの，$[k]_2^{n,i}$ は $[k]_2^n$ の下から i ビット目を指す．例えば，$[5]_2^4 = 0101$，$[5]_2^{4,1} = [5]_2^{4,3} = 1$ である．式(16)において例えば $n = 3$ の場合は，$\boldsymbol{X}_{101} = \alpha_\Gamma(V_1) \cap \overline{\alpha_\Gamma(V_2)} \cap \alpha_\Gamma(V_3)$ となる．簡単のため，以下では $\boldsymbol{X}_{[k]_2^n}$ を $\boldsymbol{X}_k$ と表記する．容易に分かるように，$\alpha_\Gamma(V_i)$，$i = 1,2,\ldots,n$ は，$\boldsymbol{X}_k$，$k = 0,1,\ldots,N$, から定まり，次の関係を満たす．

$$\boldsymbol{X}_0 = \emptyset \tag{17}$$

$$\boldsymbol{X}_k \cap \boldsymbol{X}_{k'} = \emptyset \text{ if } k \neq k' \tag{18}$$

$$\alpha_\Gamma(V_i) = \bigcup_{k:[k]_2^{n,i}=1} \boldsymbol{X}_k \tag{19}$$

$$\alpha_\Gamma(\boldsymbol{A}) = \bigcup_{k=1}^{N} \boldsymbol{X}_k - \bigcup_{\substack{k:[k]_2^{n,i}=0 \\ \text{for all } V_i \in \boldsymbol{A}}} \boldsymbol{X}_k \tag{20}$$

$$\alpha_\Gamma(\boldsymbol{V}) = \bigcup_{k=1}^{N} \boldsymbol{X}_k \tag{21}$$

式(17)から，$\boldsymbol{X}_0$ は考える必要がない．また，式(18)(20)から $|\boldsymbol{X}_k| = x_k$ と置くと，次式が成り立つ．

$$|\alpha_\Gamma(\boldsymbol{A})| = \sum_{k=1}^{N} x_k - \sum_{\substack{k:[k]_2^{n,i}=0 \\ \text{for all } V_i \in \boldsymbol{A}}} x_k \tag{22}$$

ここで，$\boldsymbol{x} = [x_1, x_2, \ldots, x_N]$ とし，ベクトル $\boldsymbol{a}(\boldsymbol{A}) = [a(\boldsymbol{A})_1, a(\boldsymbol{A})_2, \ldots, a(\boldsymbol{A})_N] \in \{0,1\}^N$ を $\boldsymbol{A} = \{V_{i_1}, V_{i_2}, \ldots, V_{i_u}\}$ に対して

$$a(\boldsymbol{A})_k = \begin{cases} 0 & \text{if } [k]_2^{n,i_1} = \cdots = [k]_2^{n,i_u} = 0 \\ 1 & \text{otherwise} \end{cases} \tag{23}$$

と定義すると，式(22)の右辺は$\boldsymbol{a}(\boldsymbol{A})\cdot\boldsymbol{x}$と書ける．最後に，$[k]_2^n$のハミング重みを$h_k$と定義し，$\boldsymbol{h}=[h_1,h_2,\ldots,h_N]$とすると，式(19)から，次式を得る．

$$\begin{aligned}\sum_{i=1}^{n}|\alpha_\Gamma(V_i)| &= \sum_{i=1}^{n}\sum_{k:[k]_2^{n,i}=1}x_k \\ &= \sum_{k=1}^{N}h_kx_k \\ &= \boldsymbol{h}\cdot\boldsymbol{x} \end{aligned} \tag{24}$$

以上から，複数割当写像の条件式(11)に式(24)を加えて，平均レート$\tilde{\rho}$を最小化する最適な複数割当写像$\tilde{\alpha}_\Gamma$を与える整数計画問題$\mathrm{IP}_{\tilde{\rho}}(\Gamma)$，および最悪レート$\rho^*$を最小化する整数計画問題$\mathrm{IP}_{\rho^*}(\Gamma)$が，それぞれ次のように定式化できる．

$\mathrm{IP}_{\tilde{\rho}}(\Gamma)$:
minimize $\boldsymbol{h}\cdot\boldsymbol{x}$

$$\begin{aligned} \text{subject to}\quad & \boldsymbol{a}(\boldsymbol{A})\cdot\boldsymbol{x}\geq t, && \text{for } \boldsymbol{A}\in\mathcal{A}_1^- \\ & \boldsymbol{a}(\boldsymbol{B})\cdot\boldsymbol{x}\leq t-1, && \text{for } \boldsymbol{B}\in\mathcal{A}_0^+ \\ & \boldsymbol{x}\geq\boldsymbol{0} \end{aligned}$$

$\mathrm{IP}_{\rho^*}(\Gamma)$:
minimize M

$$\begin{aligned} \text{subject to}\quad & \boldsymbol{a}(\boldsymbol{A})\cdot\boldsymbol{x}\geq t, && \text{for } \boldsymbol{A}\in\mathcal{A}_1^- \\ & \boldsymbol{a}(\boldsymbol{B})\cdot\boldsymbol{x}\leq t-1, && \text{for } \boldsymbol{B}\in\mathcal{A}_0^+ \\ & \boldsymbol{a}(V)\cdot\boldsymbol{x}\leq M, && \text{for } V\in\boldsymbol{V} \\ & \boldsymbol{x}\geq 0 \end{aligned}$$

ここで，$\mathcal{A}_1^-$と$\mathcal{A}_0^+$は，それぞれ，極小な有資格集合の族および極大な禁止集合の族である．

このようにして構成されたSSSは，cumulative mapを用いる従来の手法[10][11][15]に比べて，一般に小さい符号化レートを持ち，複数割当写像を用いるSSSの中で常に最適なSSSを与える．なお，上記の手法は，ランプ型のアクセス構造やアクセス構造が一部未定である不完全な一般アクセス構造に対しても，容易に拡張することができる．

4 視覚復号型秘密分散法とオーディオ秘密分散法

視覚復号型秘密分散法では，秘密画像をn個の分散画像に分散符号化し，OHPシートのような透明なシートに分散画像を印刷する．復号は，それらのシートを重ねることにより，秘密画像を見ることができる．復号に全く計算機を必要としないことが，通常の秘密分散法と大きく異なる点であり，災害時などの非常時にも秘密情報を復号できる特徴がある．ただし，復号画像は秘密画像に比べて画質がかなり劣化するため，秘密画像に細かい多くの情報を載せることは困難である．

表 3: 視覚復号型秘密分散法の種類

秘密画像の種類：白黒画像，濃淡画像，カラー画像
分散画像の種類 ：ランダムドット画像，ID 画像
秘密画像の個数：単一，複数

視覚復号型秘密分散法 (Visual Secret Sharing Scheme, VSSS) は，最初 Visual cryptography という名前で提案されたが [4]，それらは白黒画像に対する (k,n) しきい値法であった．視覚復号型秘密分散法に関しては，非常に多くの研究がなされているが，システマティックに VSSS を構成する方法として，代数的構成法がある [18][2]．この方式は，白黒画像 [19]，濃淡画像 [20]，カラー画像 [18] に適用できる．また，複数の秘密画像を 1 度に分散符号化する VSSS[21] や，分散画像に ID 画像を付ける方法 [23] などが知られている．また，カラー画像は，色の重ね合わせを利用する方法や，3 原色のみを利用する方法 [24] などがある．ここでは，紙面の都合上，詳細は省略するが，引用した論文およびそれらに記載されている参考論文を参照して欲しい．

画像の代わりに，音声や音楽などを利用したオーディオ秘密分散法も，幾つか試みられている．音波の重ね合わせにより秘密情報を作りだす方法 [5] や，リズムを音楽の中に埋め込む方法 [25] などが考えられているが，視覚型秘密分散法に比べて研究が進んでいない．

5 量子秘密分散法の符号化効率評価

量子秘密分散法 (Quantum Secret Sharing Scheme, QSSS) には，古典ビットを量子状態に分散符号化する QSSS[5][7] と，秘密量子状態を量子状態に分散符号化する QSSS[8][9] が存在するが，本節では，後者の QSSS を取り扱う．(k,n) しきい値 QSSS を量子通信路と見なすことにより，その符号化効率の限界を示す．また，その結果を，(k,L,n) しきい値ランプ型秘密分散法に拡張する．なお，本節の内容は [26] による．

5.1 量子秘密分散法の定義

$\mathcal{H},\mathcal{J},\mathcal{K},\ldots$ を有限次元 Hilbert 空間とし，密度作用素全体を $\mathcal{S}(\mathcal{H})$，純粋状態全体を $\mathcal{S}_1(\mathcal{H})$ などと表すことにする．また，量子通信路 $\mathcal{E}:\mathcal{S}(\mathcal{J})\to\mathcal{S}(\mathcal{K})$ と言った場合，$\mathcal{E}$ は完全正でトレースを保存する線形写像とする．QSSS では，Hilbert 空間 $\mathcal{H}$ 上の量子状態を，Hilbert 空間 $\mathcal{H}_i\,(i=1,\ldots,n)$ で表される複数の物理系に分散符号化する．以下では $\boldsymbol{n}\stackrel{\text{def}}{=}\{1,\ldots,n\}$ とし，$\boldsymbol{r}\subseteq\boldsymbol{n}$ に対して対応する合成物理系を $\mathcal{H}_{\boldsymbol{r}}\stackrel{\text{def}}{=}\bigotimes_{i\in\boldsymbol{r}}\mathcal{H}_i$ で表す．このとき，QSSS は量子通信路 $W_{\boldsymbol{n}}:\mathcal{S}(\mathcal{H})\to\mathcal{S}(\mathcal{H}_{\boldsymbol{n}})$ として記述される．また，$\boldsymbol{r}\subseteq\boldsymbol{n}$ に対して，量子通信路 $W_{\boldsymbol{n}}$ と部分トレース $\mathrm{Tr}_{\boldsymbol{n}\backslash\boldsymbol{r}}$ の合成量子通信路を $W_{\boldsymbol{r}}\stackrel{\text{def}}{=}\mathrm{Tr}_{\boldsymbol{n}\backslash\boldsymbol{r}}\cdot W_{\boldsymbol{n}}$

[2][18] の論文タイトルでは「解析的構成法」という用語が用いられているが，「代数的」な構造をより多く用いているため，ここでは「代数的構成法」と呼ぶ．

とおく.

定義 5 量子通信路 $\mathcal{E}:\mathcal{S}(\mathcal{J})\to\mathcal{S}(\mathcal{K})$ に対して，$\mathcal{S}$ を $\mathcal{S}(\mathcal{J})$ の部分集合とする.

1. 任意の $\rho\in\mathcal{S}$ に対して，$\mathcal{R}\cdot\mathcal{E}(\rho)=\rho$ となる量子通信路 $\mathcal{R}:\mathcal{S}(\mathcal{K})\to\mathcal{S}(\mathcal{J})$ が存在するとき，量子通信路 $\mathcal{E}$ は $\mathcal{S}$ に関して可逆であるという.

2. 任意の $\rho\in\mathcal{S}$ に対して，$\mathcal{E}(\rho)=\rho_0$ となる $\rho_0\in\mathcal{S}(\mathcal{K})$ が存在するとき，量子通信路 $\mathcal{E}$ は $\mathcal{S}$ に関して消失的であるという.

一般の量子通信路に対する上記の定義を用いて，QSSS における有資格集合と禁止集合，および完全な QSSS とランプ型 QSSS を次のように定義する.

定義 6 $\boldsymbol{r}\subseteq\boldsymbol{n}$ に対して，$W_{\boldsymbol{r}}$ が $\mathcal{S}_1(\mathcal{H})$ に関して可逆 (resp. 消失的) であるとき，$\boldsymbol{r}$ は有資格集合 (resp. 禁止集合) であるという.

定義 7 QSSS $W_{\boldsymbol{n}}$ に関して，すべての $\boldsymbol{r}\subseteq\boldsymbol{n}$ が有資格集合または禁止集合であるとき，$W_{\boldsymbol{n}}$ を完全な QSSS と呼ぶ．そうでない場合，$W_{\boldsymbol{n}}$ をランプ型 QSSS と呼ぶ.

QSSS $W_{\boldsymbol{n}}$ が，任意の $\rho\in\mathcal{S}_1(\mathcal{H})$ に対して $W_{\boldsymbol{n}}(\rho)\in\mathcal{S}_1(\mathcal{H}_{\boldsymbol{n}})$ となるとき，$W_{\boldsymbol{n}}$ を pure state QSSS といい，そうでない場合，$W_{\boldsymbol{n}}$ を mixed state QSSS という．このとき，次の補題が成立するため，pure state QSSS を考えれば十分である．なお，[9] においては完全な QSSS に対して証明されているが，ランプ型 QSSS に対しても成立する.

補題 8 (Gottesman[9]) 任意の mixed state QSSS $W_{\boldsymbol{n}}$ は，pure state QSSS $W_{\boldsymbol{n}'}$ において一部の系を取り除いた部分系として実現できる．また，QSSS $W_{\boldsymbol{n}'}$ のアクセス構造は元の $W_{\boldsymbol{n}}$ のアクセス構造から一意に定まる.

5.2 量子秘密分散法の符号化効率

量子状態の集合 $\mathcal{S}\subseteq\mathcal{S}(\mathcal{J})$ 上のいたるところで正の重みを持つ確率測度全体を $\mathcal{P}_+(\mathcal{S})$ とおく．また，$\mu\in\mathcal{P}_+(\mathcal{S})$ に関する平均操作を $\mathrm{E}_\mu\big[\rho\big]=\int_{\mathcal{S}}\rho\,\mu(\mathrm{d}\rho)$ と書くことにする．量子状態アンサンブル $\mu\in\mathcal{P}_+(\mathcal{S})$ が与えられたとき，μ に関する確率的混合状態を $\sigma_\mu\stackrel{\mathrm{def}}{=}\mathrm{E}_\mu\big[\rho\big]$ とおく．このとき，Holevo 相互情報量は μ と量子通信路 $\mathcal{E}$ に対して次式で定義される.

$$\begin{aligned} I(\mu;\mathcal{E}) &\stackrel{\mathrm{def}}{=} \mathrm{E}_\mu\big[D(\mathcal{E}(\rho)||\mathcal{E}(\sigma_\mu))\big] \\ &= H(\mathcal{E}(\sigma_\mu))-\mathrm{E}_\mu\big[H(\mathcal{E}(\rho))\big] \end{aligned} \tag{25}$$

ただし，$H(\rho)\stackrel{\mathrm{def}}{=}-\mathrm{Tr}\big[\rho\log\rho\big]$ は von Neumann エントロピーである．このとき，一般の量子通信路に関して次の定理が成り立つ.

定理 9 量子通信路 $\mathcal{E}:\mathcal{S}(\mathcal{J})\to\mathcal{S}(\mathcal{K})$ と $\mathcal{S}\subseteq\mathcal{S}(\mathcal{J})$ が与えられているとき，次の 3 つ条件は同値である．ただし，$\mathcal{I}$ は恒等写像 $\mathcal{I}:\rho\in\mathcal{S}(\mathcal{J})\mapsto\rho\in\mathcal{S}(\mathcal{J})$ である.

1 : $\mathcal{E}$ は $\mathcal{S}$ に関して可逆 (resp. 消失的)

2 : $\forall \mu \in \mathcal{P}_+(\mathcal{S})$, $I(\mu;\mathcal{E}) = I(\mu;\mathcal{I})$ (resp. $= 0$)

3 : $\exists \mu \in \mathcal{P}_+(\mathcal{S})$, $I(\mu;\mathcal{E}) = I(\mu;\mathcal{I})$ (resp. $= 0$)

$\mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H}))$ に関する $W_{\boldsymbol{r}}(\rho)$ の確率的混合状態は $\mathrm{E}_\mu\big[W_{\boldsymbol{r}}(\rho)\big] = W_{\boldsymbol{r}}(\sigma_\mu)$ で与えられる．純粋状態 ρ に対しては $H(\rho) = 0$ であるので，純粋状態アンサンブル $\mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H}))$ に対する Holevo 相互情報量は $I(\mu;\mathcal{I}) = H(\sigma_\mu) - \mathrm{E}_\mu\big[H(\rho)\big] = H(\sigma_\mu)$ となる．よって定理 9 の $\mathcal{E}$ として，$W_{\boldsymbol{r}}(\rho)$ を考えると，QSSS に対して次の定理が得られる．

定理 10 QSSS $W_{\boldsymbol{n}}$ が与えられているとき，$\boldsymbol{r} \subseteq \boldsymbol{n}$ に対して以下は同値である．

1 : $\boldsymbol{r}$ は有資格集合 (resp. 禁止集合)

2 : $\forall \mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H}))$, $I(\mu;W_{\boldsymbol{r}}) = H(\sigma_\mu)$ (resp. $= 0$)

3 : $\exists \mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H}))$, $I(\mu;W_{\boldsymbol{r}}) = H(\sigma_\mu)$ (resp. $= 0$)

系 $\boldsymbol{r}(\subseteq \boldsymbol{n})$ が無意味でない場合，$\boldsymbol{r} \cup \boldsymbol{u}$ が有資格集合となるような禁止集合 $\boldsymbol{u}(\subseteq \boldsymbol{n})$ が必ず存在するが，そのような系 $\boldsymbol{r}$ を有用な系と呼ぶ．このとき，定理 10 を用いて次の定理を導くことができる．

定理 11 QSSS $W_{\boldsymbol{n}}$ における有用な系 $\boldsymbol{r}$ に対して，以下の不等式が成立する．

$$, H(\sigma_\mu) \leq H(W_{\boldsymbol{r}}(\sigma_\mu)) \text{ for } \forall \mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H})), \tag{26}$$

これは，Nascimento らの結果 [27] と一致する．また，定理 11 において，μ を一様分布に選ぶことにより，任意の有用な系 $i \in \boldsymbol{n}$ に対して，

$$\dim \mathcal{H} \leq \dim \mathcal{H}_i \tag{27}$$

が成り立つ．これは，Gottesman[9] の結果に一致する．

5.3 ランプ型秘密分散法と符号化効率限界

QSSS のアクセス構造が以下の条件を満たすとき，(k, L, n) しきい値ランプ型 QSSS であるという．

$$|\boldsymbol{r}| \leq k - L \quad \Leftrightarrow \quad \boldsymbol{r} \text{は禁止集合} \tag{28}$$

$$|\boldsymbol{r}| \geq k \quad \Leftrightarrow \quad \boldsymbol{r} \text{は有資格集合} \tag{29}$$

また，$L = 1$ の場合を (k, n) しきい値 QSSS という．このとき，次の定理が成り立つ．

定理 12 (k, L, n) しきい値ランプ型 QSSS では，$n \leq 2k - L$ の関係が成立する．特に pure state QSSS の場合は $n = 2k - L$ が成立する．

この定理は，[8] で示された (k,n) しきい値法に対する結果の拡張となっている．(k,L,n) しきい値ランプ型 QSSS に対して，定理 11 の証明と同様の手法により次の定理を証明できる．

定理 13 (k,L,n) しきい値ランプ型 QSSS においては以下の不等式が成立する．

$$\forall \mu \in \mathcal{P}_+(\mathcal{S}_1(\mathcal{H})),\ \frac{1}{L}H(\sigma_\mu) \leq \frac{1}{n}\sum_{i\in \boldsymbol{n}} H(W_i(\sigma_\mu)) \tag{30}$$

μ が一様分布の場合を考えると，

$$\frac{1}{L}\dim \mathcal{H} \leq \frac{1}{n}\sum_{i\in \boldsymbol{n}} \dim \mathcal{H}_i \tag{31}$$

が成り立つ．これらの結果は，$L=1$ のとき，(k,n) しきい値 QSSS の結果（定理 11）に一致する．定理 11,13 より，(k,L,n) しきい値ランプ型 QSSS は，(k,n) しきい値ランプ型 QSSS よりも，符号化効率が平均で L 倍よくなる．

参考文献

[1] Shamir, A.: How to share a secret, Comm. Assoc. Comput. Mach., vol.22, no.11, pp.612 613 (Nov. 1979)

[2] E.D.Karnin, J.W.Greene, M.Hellman, "On secret sharing systems,"" IEEE Trans. on Inform. Theory, vol.IT-29, no.1, pp.35–41, Jan. 1983

[3] , Y.Kawamoto and H.Yamamoto, "Secret function sharing schemes and their applications on the obvious transfer," IEEE-ISIT2003, June 30-July 4, 2003, Yokohama, Japan

[4] M.Naor and A.Shamir, "Visual cryptograph," Advances in Cryptology, EUROCRYPT'97, LNCS 950, Springer-Verlag, pp.1-12, 1994

[5] Y.Desmedt, S.Hou, J.-J.Quisquater, "Cerebral cryptography, " Proc. of Information Hinding, LNCS 1525, Springer-Verlag, pp.62-72, 1998

[6] M.Hillery, V.Buzek, and A.Berthiamue, "Quantum secret scheme," Los Alamos e-print archive, no.quant-ph/9806063, 1998

[7] A.Karlsson, M.Koashi, and N.Imoto, "Quantum entanglement for sharing secret splitting," Physical Review A, vol.59, no.1, pp.162-168, 1999

[8] R.Cleve, D.Gottesman, and H.-K.Lo, "How to share a quantum secret," Physical Review Letters, vol.83, no.3, pp.648-651, 1999

[9] D.Gottesman, "Theory of Quantum secret sharing," Physical Review A, vol.61, no.042311, 2000

[10] 伊藤, 斎藤, 西関, "一般的なアクセス構造を実現する秘密共有法," 電子情報通信学会論文誌, vol.J71-A, no.8, pp.1592-1598, 1988

[11] M.Itoh, A.Saito and T.Nishizeki, "Multiple assignment scheme for sharing secret," *J. of Cryptology*, vol.6, pp.15-20, 1993

[12] 山本博資, "秘密分散通信システムに対する実用暗号化法," 電子通信学会技術報告, no.IT84-8, pp.23-29, May 1984

[13] 山本博資, "(k,L,n) しきい値秘密分散システム", 電子通信学会論文誌, vol.J68-A, no.9, pp.945-952, Sep. 1985, [英訳: Electronics and Communications in Japan, Part I, vol.69, no.9, pp.46-54, (Scripta Technica, Inc.), Sep. 1986]

[14] G.R.Blakley and C.Meadows, "Security of ramp schemes," Advances in Cryptology-Crypto'84, LNCS196, Springer-Verlag, pp.242-269, 1985

[15] 栃窪, "一般のアクセス構造を実現する秘密情報に関する二, 三の考察," *Proc. of SCIS2001*, pp.799-804, 2001

[16] 岩本, 山本, 小川, "(k,n) しきい値法と整数計画法による秘密分散法の一般的構成法," 電子情報通信学会技術報告 SEC2003-11, pp.63-70, 2003

[17] M.Iwamoto, H.Yamamoto, H.Ogawa, "Optimal multiple assignment based on integer programming for secret sharing schemes with general access structures," (submitted to *J. of Cryptology*)

[18] H.Koga, M.Iwamoto, and H.Yamamoto, "An analytic construction of the visual secret sharing scheme for color images," IEICE Trans. on Fundamentals, vol.E84-A, no.1, pp.262-272, Jan. 2001

[19] H.Kuwakada and H.Tanaka,"Polynominal representation of visual secret sharing scheme and its application," IEICE Trans. on Fundamentals, vol.E85-A, no.6, pp.1379-1386, 2002

[20] M.Iwamoto and H.Yamamoto, "The optimal n-out-of-n visual secret sharing scheme for gray-scale images," IEICE Trans. on Fundamentals, vol.E85.A, no.10, pp.2238-2247, Oct. 2002

[21] M.Iwamoto and H.Yamamoto, "A construction method of visual secret sharing schemes for plural secret images," *IEICE Trans. on Fundamentals*, vol.E86-A, no.10, pp2577-2588, 2003

[22] M.Iwamoto and H.Yamamoto, "Visual Secret Sharing Schemes for Plural Secret Images," *Proc. of IEEE ISIT2003*, p.283, 2003

[23] T.Ishihara and H.Koga, "New constructions of the latteice-based visual secret sharing using mixture of colors," IEICE Trans. on Fundamentals, vol.E-85-A, no.1, pp.158-166, 2002

[24] T.Ishihara and H.Koga, "A visual secret sharing scheme for color images based on meanvalue-color mixing," IEICE Trans. on Fundamentals, vol.E-86-A, no.1, pp.194-197, 2003

[25] S.-Y.Chiou and C.-S.Laih,"A tempo-based audio cryptography scheme," IEICE Trans. on Fundamentals, vol.E-86-A, no.8, pp.2091-2098, 2003

[26] 小川, 佐々木, 岩本, 山本, "量子秘密分散法の符号化効率評価と構成法, 第26回情報理論とその応用シンポジウム (SITA2003) 予稿集, pp.651-654, 2003

[27] C. A. Nascimento, Hideki Imai, "A quantum information theoretical model for quantum secret sharing schemes," *Proc. of EQIS 2001*, Tokyo, Japan, September, 2001.